STATINTL

NOTE TO: [redacted]

FROM:

SUBJECT: Guidelines for National Security Classification

You asked for my ideas on the subject of classification management guidance and here they are (attached). It occurred to me that what is going to be necessary for publication in the Federal Register or for eventual submission to ISOO is a statement of policy and intent in addition to a checklist of those "information elements to be protected..." Much information is floating about and I sought to bring it together as a statement of policy in an area where the CIA will surely be questioned. The sources of my draft are DOD 5200.1-R (Information Security Program Regulation, a 102-page public document), E.O. 12065, and those portions

STATINTL

of the largely obsolete HR [redacted] which will have continued applicability. In its present format, I believe that further additions concerning lines of security classification authority, marking, and finally the list of "information elements" could be added as they are developed. I am probably not qualified to judge the criteria for classifying sources or methods but I think the statements I have prepared on the attached would serve as a basic policy declaration to be expanded upon.

GUIDELINES FOR THE EXERCISE OF NATIONAL SECURITY CLASSIFICATION

I. INTRODUCTION

1. Executive Order 12065 of 3 July 1978 and its Implementing Directive of _____ mandates all Executive Branch agencies to establish guides for determing the level of classification at which national security sensitive official documents, information, and/or material are to be protected and for what length of time.

2. The following guidelines apply to all official documents, information, and material originated by or attributable to any component of the Central Intelligence Agency which contain national security sensitivities requiring a degree of protection from unauthorized or improper disclosure in accordance with statute, Executive Order, or current CIA regulations, or which place an individual in immediate jeopardy.

3. The purpose of this guideline is to establish the criteria for insuring that the official documents, information, and material originated by or attributable to the CIA and/or its components which require a national security classification shall be protected to the extent and for the period necessary. The provisions of this guideline may be made applicable, by contract or other legally binding instrument, to non-governmental individuals, organizations, and entities entrusted with national security classified documents, information, and material.

4. Nothing in this guideline supercedes restrictions imposed by the Atomic Energy Act of 1954 (as amended), the Patent Secrecy Act of 1952,

other statutes, Executive Orders, and restrictions imposed by the originators of official documents, information, and material over which the CIA does not exercise original or final authority.

II. DEFINITIONS

1. Classification - see national security classification.

2. Classified Information - see national security sensitive information.

3. Classifier - An individual who either:

a. determines that official information, not known by him to be already classified, currently requires, in the interests of national security, a specific degree of protection against unauthorized disclosure and having the authority to do so, designates that official information as Top Secret, Secret or Confidential; or

b. determines that official information is in substance the same as information known by him to be already classified by the government as Top Secret, Secret or Confidential and designates it accordingly.

4. Component - the offices of the Director and Deputy Director of Central Intelligence; the independent offices; the Directorates of Administration, Operations, and Science and Technology; the National Foreign Assessment Center; and all supporting or subordinate offices, divisions, and staffs.

5. Compromise - the known or suspected exposure of national security classified documents, information or material to an unauthorized person.

6. Custodian - the individual or component who has possession of or is otherwise charged with the responsibility for safeguarding and accounting for national security classified information.

7. Document (or Record) - recorded information regardless of medium or characteristics as defined by 44 USC 3301.

8. Foreign Government Information - information that has been provided to the United States in confidence by, or produced by the United States pursuant to a written joint arrangement requiring confidentiality with a foreign government, or international organization of governments.

9. Immediate Jeopardy - the placing of an individual in danger of immediate physical or severe political harm or reprisal.

10. Information - the content of any document (or record) which can be communicated by any means.

11. Material - product, substance, item of equipment, or other physical objection or in which information may be recorded or embodied.

12. Method (of Intelligence) - the means used to provide support to an intelligence source or operation and which, if disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in supporting foreign intelligence or counterintelligence activities or which could, if disclosed, reasonably lead to the disclosure of an intelligence source or operation.

13. National Security - collective term encompassing both the national defense and foreign relations of the United States.

14. National Security Classification - the determination that official information requires a specific degree of protection against unauthorized disclosure in the interests of national security and/or the safeguarding of individuals from personal jeopardy.

15. National Security Sensitive Information - official information which has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

16. Official Information - information which is owned by, produced for or by, or is subject to the control of the CIA or any other agency of the United States Government as defined in 5 U.S.C. 552(f).

17. Original Classification Authority - the authority to make original national security classifications which is vested specifically and in writing in an official of the CIA as the incumbent of an office, and in the official specifically and in writing designated to act in the absence of the incumbent.

18. Source -

a. a person, organization, or technical means which provides foreign intelligence and/or counterintelligence and which, if its identity or capability is disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness, or

b. a person or organization which provides foreign intelligence and/or counterintelligence to the United States only on the condition that its identity remains undisclosed.

III. SECURITY CLASSIFICATION CATEGORIES

1. TOP SECRET - the category of national security sensitive information which requires the highest degree of protection because its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples include armed hostilities against the United States or its allies; disruption of foreign relations

vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

2. SECRET - the category of national security sensitive information which requires a substantial degree of protection because its unauthorized disclosure could reasonably be expected to cause serious damage to the national security or place an individual in immediate jeopardy. Examples of serious damage include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security, revelation of significant military plans or intelligence operations; compromise of significant scientific or technological developments relating to national security; or the identification of human intelligence sources in such a fashion as to make the sources and/or their family and immediate descendants vulnerable to physical or severe political harm or reprisal.

3. CONFIDENTIAL - the category of national security sensitive information which requires a degree of protection because its unauthorized disclosure could reasonably be expected to cause identifiable damage to the national security.

IV. CLASSIFICATION POLICY

1. Except as expressly provided by statute, no national security classification category other than III (1)-(3) shall be used to identify official documents, information, and material requiring protection in the interests of national security, or safeguarding individuals from personal

jeopardy.

2. Subject to the prior specific approval of the Deputy Director for Administration, special measures, including compartmentation systems, may be imposed with respect to controlling access, distribution and protection of national security classified official documents, information, and material including those which relate to communications intelligence, intelligence sources and methods, and cryptography. Special measures in existence on the effective date of E.O. 12065 and its Implementing Directive remain valid without reissuance or reapproval.

3. National security classified foreign grovernment information shall either retain its original classification designation or be assigned a United States classification designation that shall ensure a degree of protection equivalent to that required by the entity that furnished the information. The unauthorized disclosure of foreign government information or the identity of a foreign source requiring protection is presumed to cause at least identifiable damage to the national security.

4. Classification determinations must be preceded by an exact identification of each item of information which may require security protection. This process involves the identification of that specific information which possesses a national security sensitivity or which is reasonably believed to place an individual in immediate jeopardy. Each security classified document shall indicate clearly which portions require a national security classification, the applicable level of classification, and which portions are not security classified.

5. An evaluation of information forms the basis for national security classification. A document or other material is given a national

security classification either (1) because the information which it contains may be determined by study, analysis, observation, or use; or (2) because of the information it may reveal when associated with other information, including that which the classifier knows already has been officially released into the public domain. Intelligence operations inherently involve a mosaic of information in which isolated and apparently unrelated items can be linked together to reveal or endanger intelligence sources and mathods. By statute, the Director of Central Intelligence is responsible for protecting intelligence sources and methods from unauthorized disclosure.

6. The state-of-the-art in other nations, and/or by international organizations or non-national entities is a vital factor to be considered in national security classification determinations. Such determinations of national security classification require consideration of the information available from intelligence sources concerning the extent to which the same or similar information is known or is available to others. It is also important to consider whether it is known, publicly or internationally, that the United States has the information or is even interested in the subject matter.

7. Whenever a subject, program, operation, or project has been classified by the Director, a Deputy Director, or another official authorized to make that decision (including non-CIA officials) that decision controls the decisions of all other persons with respect to any documents of a substantive nature originated by them involving such matter.

8. The degree of intended or anticipated dissemination and use, and whether the end purpose to be served would render effective security control factors impractical are factors to be considered in determining whether a

national security classification is to be imposed and at what level. These factors do not necessarily preclude security classification but they require consideration of the extent to which national security classification under such circumstances may degrade the security classification system by attempting to impose security control in impractical situations. Determinations dependent upon such factors are the responsibility of the official having original classification authority over the documents, information, or material involved.

9. Each document shall be security classified on the basis of the information which it contains or reveals. The overall classification of a document shall be as high as that of its most highly classified portion. Each portion shall be security classified individually on its own merits. Persons who prepare security classified documents by abstracting or synopsizing other security classified information from multiple sources shall apply the highest security classification used in such sources, if such a classification is warranted in the finished document.

10. Files, containers, and other items which contain documents and/or materials shall be classified at least as high as that of the most highly classified component therein. When it is feasible to do so, documents of differing national security classifications should not be physically connected.

11. Non-documentary material may be security classified when security classified information can be derived from it by visual observation of internal or external appearance, structure, operation, test, application, or use. The overall security classification assigned to such material shall be at least as high as the highest classification of any of the items of information revealed.

12. Appearance in the public domain of information currently carrying, or being considered for, a national security classification does not preclude initial or continued classification; however, such disclosures require immediate re-evaluation of the information to determine whether the publication has so compromised the information that further security classification at its existing level is warranted. Similar consideration must be given to related items of information in all programs, projects or items incorporating or pertaining to the compromised items of information. Custodians of compromised security classified information should continue classification until advised to the contrary by competent authority.

13. National security classified documents, information, and material shall be handled in accordance with current CIA regulations for the handling, storage, referencing, dissemination, use, and destruction of such items. Access to national security classified documents, information, and material shall be based upon the appropriate security clearance and the need of the person to have access in order to perform his/her official duties or contractual obligations.

Any employee who has knowledge of the loss or possible compromise of classified information or documents shall immediately report the circumstances to the Director of Security. The Director of Security shall notify all interested departments and agencies in order that a damage assessment may be conducted. If the loss or compromise occurred in CIA, the Director of Security immediately shall initiate an inquiry for the purpose of taking corrective measures and recommending appropriate administrative, disciplinary or legal action.

V. CLASSIFICATION RESTRICTIONS

1. National security classification shall apply only to official information requiring protection in the interests of national security and the safeguarding of individuals from immediate jeopardy. It may not be used to conceal violations of law, inefficiency or administrative error, to prevent embarrassment, or to restrain competition.

2. When determined to be necessary, national security classification shall be retained for the minimum length of time considering the degree of sensitivity, cost, and probability of compromise. Unnecessary security classification shall be scrupulously avoided.

3. Basic scientific research not clearly related to the national defense, or the product of non-governmental research and development that does not incorporate or reveal security classified information to which the producer or developer was given prior access, may not be security classified.

4. References to security classified documents, that do not, standing alone, reveal security classified information, may not themselves be security classified, or be used as the basis for security classification.

5. Compilations, abstracts, and/or synopses of unclassified documents or information may not be classified unless they contain additional information in their final format which is otherwise subject to national security classification. Such additional information shall be clearly designated with the appropriate national security classification.